平成 21 年度事後事業評価書

政策所管部局課室名 総合通信基盤局電気通信事業部データ通信課
評価年月：平成２１年７月

1 政策 (事業等名称)

電気通信事業分野におけるサイバー攻撃対応演習

2 達成目標

サイバー攻撃等によってインターネットのセキュリティが侵害される事案（以下「インシデント」という。）に対応するためには、事業者内・事業者間連携に関する課題を抽出し、その課題について共通認識を持つことが重要であり、それを達成目標として本事業が実施された。

（課題として想定されるもの）

・事業者間連携体制の整備が必要。

・顧客・事業者間においてインシデント対応に関する具体的な取り決めが必要。

・インシデントに対応可能な人材の育成が必要。

本事業の実施後においては、本事業によって明らかとなった課題を各参加者が現状の体制や組織の運営状況等、各自の特性を考慮した上で、各自の判断により自社のサイバー攻撃対応体制等に反映させることにより、インターネットの安全性・信頼性の向上が図られ、利用者が安心・安全にインターネットを利用できる環境が実現されることが期待できる。

3 事業等の概要等

（1）事業等の概要

・実施期間

平成１８年度から平成２０年度

・実施主体

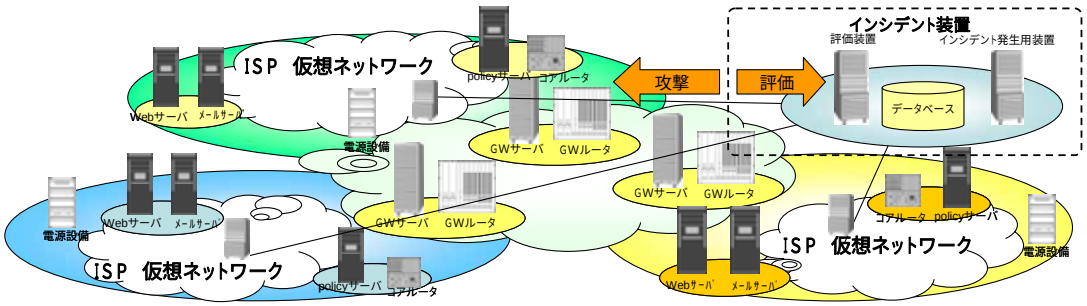
民間企業

・概要

ネットワークの安心・安全な利用環境の実現に向けて、サイバー攻撃等によるインターネットのインシデントに対応する演習を行うことにより、高度な IT スキルを有する人材を育成し、かつ事業者内・事業者間の連携体制を強化する。

・概要図

○　演習環境イメージ



仮想ネットワーク環境

・総事業費

（単位：百万円）

事業年度	１８年度	１９年度	２０年度	総事業費
予算額	４０４	３６２	３２６	１，０９２

（２）事業等の必要性及び背景

インターネットは、国民の社会経済活動を支えるインフラとして定着し、その重要性が高まる一方、本事業の開始当初において、ネットワークに接続しただけで感染してしまうコンピューターウイルスや多数のコンピュータから一斉に攻撃が行われる事案が発生していた。

こうしたインシデントの広域化や組織的攻撃により、個々の電気通信事業者のみでは対応できなくなっていたことから、事業者間及び事業者と行政との間で連携してセキュリティ対策を講じることのできる人材や協力体制の強化が求められる等、社会的にも演習の実施に関するニーズが高まっていた。

また、「情報セキュリティ基本問題委員会 第 2 次提言」（平成 17 年 4 月、ＩＴ戦略本部）において、演習等を通じて高度なＩＴスキルを有する人材を育成すべきと提言されている他、「次世代 IP インフラ研究会 第二次報告書」（平成 17 年 7 月、総務省）においても、インシデント事案の広域化や組織的攻撃の増加という当時の傾向にかんがみ、事業者をまたがる総合的な演習の必要性を提言している等、様々な政策提言において演習の実施の必要性が指摘されている。

さらに、本事業は事業者をまたがるサイバー攻撃対応演習を実施するものであり、電気通信事業者、Web サービス提供事業者等複数の事業者を想定した、大規模な演習環境の構築が必要であった。しかしその一方で、事業者にとっては、利害の対立する事業者間において自主的に演習に取り組むことが困難であったこと、いつ起こるか分からないサイバー攻撃への対応演習に費用をかけにくいという実情もあったことから、まずは国費を投じて演習環境を構築し、サイバー攻撃対応演習を実施することが必要であった。

（3）関連する政策、上位計画・全体計画等

○上位の政策：

政策１３「情報通信技術利用環境の整備」

○「e-Japan戦略Ⅱ」（平成１５年７月 ＩＴ戦略本部）

「情報セキュリティを確保し、不正アクセス、（中略）その他の不正行為に対処するための対策を推進」及び「情報セキュリティ全般に関する十分な知識・技術を有する専門家を育成」することとされている。

○「u-Japan政策」（平成１６年１２月 総務省）

「サイバーテロや災害・停電等により機能が停止しやすいという脆弱性を内包したネットワークはシステミックリスクにさらされており、その運用上、適切なセキュリティ対策を施すなど、十分な危機管理を行う必要がある。」こととされている。

○「情報セキュリティ基本問題委員会 第２次提言 ～我が国の重要インフラにおける情報セキュリティ対策の強化に向けて～」（平成１７年４月 ＩＴ戦略本部）

「毎年度ごとにテーマを決めた「総合的訓練・演習」の企画・実施」や「演習・訓練及びセミナー等を通じた、高度なＩＴ人材の育成」が挙げられている。

○「経済財政運営と構造改革に関する基本方針２００５」（平成１７年６月 経済財政諮問会議）

「官民における統一的・横断的なセキュリティ対策を推進する。」、「ネットワーク分野について、２０１０年までにユビキタスネット社会を実現するために、「u-Japan政策」を推進する。」及び「ＩＴを活用した安心・安全への取組を推進する。」こととされている。

○「次世代IPインフラ研究会 第二次報告書 ～「情報セキュリティ政策２００５」の提言～」（平成１７年７月 総務省）

「事業者をまたがる総合的な演習の必要性」が提言されている。

○重要インフラの情報セキュリティ対策に係る行動計画（平成１７年１２月 情報セキュリティ政策会議）

「想定される具体的な脅威シナリオの類型をもとに、毎年度テーマを設定し、各重要インフラ所管省庁、各重要インフラ事業者等、各重要インフラ分野のＣＥＰＴＯＡＲ等の協力を得て、重要インフラ分野横断的な演習を行うこととする」とされている。

○「第一次情報セキュリティ基本計画」（平成１８年２月 情報セキュリティ政策会議）

「政府は、２００９年度初めには、重要インフラにおけるＩＴ障害の発生を限りなくゼロにすることを目指す」こととされている。

○「セキュア・ジャパン2006」（平成１８年６月情報セキュリティ政策会議）

「セキュア・ジャパン2007」（平成１９年６月情報セキュリティ政策会議）

「セキュア・ジャパン2008」（平成２０年６月情報セキュリティ政策会議）

「2008年度までに、緊急時における関係事業者間および事業者・政府間の連携体制の強化や調整力を発揮できる高度なICTスキルを有する人材の育成を図るため、（中

略）電気通信事業者を中心に各重要インフラに跨るインターネット上で発生するサイバー攻撃を想定したサイバー攻撃対応演習を実施する」こととされている。

4　政策効果の把握の手法

本事業は、演習参加者全員が演習結果を個別に評価した上で課題を抽出し共通認識を得る、という手順で実施するものであり、その結果を評価することによって、政策効果を把握することとした。

具体的には本事業の結果に基づいて、本事業を有効性、効率性、公平性、優先性、及び、今後の課題及び取組の方向性の観点から評価することにより、政策効果を把握した。

5　目標の達成状況

演習を実施した後、演習参加者全員が演習結果を評価したところ、以下のとおり達成目標に掲げる（課題として想定されるもの）に類似した課題等が抽出され、共通認識として得られた。本事業の達成目標は、“共通認識を得る”という定性的なものであることから「どの程度」達成できたか測ることは難しいが、サイバー攻撃対応演習専門家として本事業の効果的な実施に協力を得たErnest W. Drew, Ⅲ氏（米国ノルウィッチ大学　サイバーコンフリクト研究所）に本事業の結果を提示し、「３年間の演習によって着実に成果をあげてきた」という評価を受けている。

＜達成目標に掲げる課題「事業者間連携体制の整備が必要」に類似した評価結果＞

〇課題

・事業者間でインシデント対応事例の情報を蓄積・共有することが必要。
・インシデント発生時の事業者内、事業者間の情報連携について再考が必要。

〇３年間の演習を通じた課題の解決状況

・演習を通して、日頃は交流の少ない事業者間で交流が生まれた。これによって有事の際の連携力の強化を図ることができた。
・情報共有は、共有に関するルールの整備や、第三者機関の利用等、環境を整えることにより、潤滑に行える可能性を見出すことができた。
・演習を通じて、自社のみで解決できない問題について他の事業者に解決を依頼する、という事業者間の連携体制を経験することによって、大規模な攻撃被害に対する対応能力が身につくと分かった。

＜達成目標に掲げる課題「顧客・事業者間においてインシデント対応に関する取り決めが必要」に類似した評価結果＞

〇課題

・顧客・事業者間において、インシデント対応に関する合意事項や連絡窓口を整備する

ことが必要。

＜達成目標に掲げる課題「インシデントに対応可能な人材の育成が必要」に類似した評価結果＞

○課題

・今後も演習を継続し、多くのオペレータにサイバー攻撃対応の経験を積んでもらうことが必要。

○３年間の演習を通じた課題の解決状況

・演習に参加したことでインシデント対応の一連の流れが確認できた。

・インシデント発生時に冷静かつ速やかに対処できる自信がついた。

6　目標の達成状況の分析

（1）有効性の観点からの評価

達成目標どおり、演習結果を参加者の中で評価し、抽出した課題を共通認識として持つことができたため、本事業は有効性があると認められる。

また３年間の演習を通じて、「５　目標の達成状況」のとおり、この課題を解決することができたと見られる参加者らもいたことから、本事業はインターネットの安全性・信頼性の向上に確実に寄与することを通じ、国民一般に対してもその結果が及ぶ有効なものであるといえる。

（2）効率性の観点からの評価

複数の事業者に跨って発生するインシデントに対して、各事業者がそれぞれの方針で対応策を講じる場合、その費用対効果は不安定なものになると考えられる。本事業はインターネットを形成する主要な電気通信事業者の多数参加を得て、インシデント対応時の課題について共通認識を持つことを目的とするものであり、共通認識としてその課題を持つ事業者らが相互に連携して解決することが期待される。したがって、本事業は確実にインターネット全体に効果が表れる効率性の高い事業である。

（3）公平性の観点からの評価

（２）のとおり、本演習を通じて共通認識となった課題の解決に対して、演習に参加した事業者が相互に連携して取り組むことは、インターネット全体に効果を発揮するものと考えられる。したがって、本事業において社会インフラとしてのインターネットの安全性・信頼性の確立に寄与することを通じ、その効果が広く国民一般に及ぶものである。

（4）優先性の観点からの評価

インシデントの広域化や組織的攻撃の増加という本事業の開始当初の状況にかんがみると、既に発生している攻撃や今後発生しうる攻撃に対応するため、速やかに対応を図る必要があり優先性があると認められる。

（5）今後の課題及び取組の方向性

本事業では、演習が民間主導で継続して実施することができるよう、演習の設計方法及び実施方法を取りまとめ、演習フレームワークを策定したことから、本事業の終了後においても、民間企業が主体となって当該演習フレームワークを活用した演習を継続して実施することが可能となった。そのため、今後は民間主導によって積極的に演習が実施されることが期待できる。

7　政策評価の結果

本事業を実施した結果、有効性、効率性、必要性、公平性及び優先性の観点から十分な成果が得られたと認められる。

一方、演習を通じて明らかになった課題の解決を図るため、今後においても、関係者は引き続き演習の実施に努めることが重要であり、そのような取組を通じてインターネットの安全性・信頼性の向上を図り、利用者が安心・安全にインターネットを利用できる環境の実現に努めるべきである。

8　学識経験を有する者の知見の活用に関する事項

本事業の評価を実施するにあたり、サイバー攻撃対応演習専門家 Ernest W. Drew, Ⅲ氏（米国ノルウィッチ大学　サイバーコンフリクト研究所）から、３年間の演習の結果について得られたコメントを活用した。

（以下、該当するコメント）

サイバー攻撃対応演習への参加者の多くはプログラムが始まった３年前には演習に参加した経験がなかった。ISP や総務省を始め様々な連携が不可欠なほど複雑なサイバー攻撃に関する問題を討議しなかった。この演習によって複雑なサイバー攻撃に対処する能力は向上している。この３年間は技術以外に事業者が連携してサイバー攻撃対応を可能にするポリシーや手順に注意を払ってきた。それによって、ISP 間の連携を重視することで総務省の施策であるこの演習は日本のサイバーセキュリティの向上に貢献してきた。脅威は今後も複雑化し進化するがサイバー攻撃対応演習を継続すれば新しい脅威への効果的な対応も可能になる。

9　評価に使用した資料等

○　e-Japan 戦略Ⅱ（平成１５年７月　ＩＴ戦略本部）
（http://www.kantei.go.jp/jp/singi/it2/kettei/030702ejapan.pdf）
○　u-Japan 政策（平成１６年１２月　総務省）
○「情報セキュリティ基本問題委員会　第２次提言　～我が国の重要インフラにおける情報セキュリティ対策の強化に向けて～」（平成１７年４月　ＩＴ戦略本部）
（http://www.nisc.go.jp/itso/kaigi/kihon/teigen/pdfs/2teigen_hontai.pdf）
○　経済財政運営と構造改革に関する基本方針２００５（平成１７年６月　経済財政諮問会議）
（http://www.kantei.go.jp/jp/singi/keizai/kakugi/050621honebuto.pdf）
○　次世代 IP インフラ研究会第二次報告書（平成１７年７月　総務省）
○重要インフラの情報セキュリティ対策に係る行動計画（平成１７年１２月　情報セキュリティ政策会議）
（http://www.nisc.go.jp/active/infra/pdf/infra_rt.pdf）
○「第一次情報セキュリティ基本計画」（平成１８年２月　情報セキュリティ政策会議）
（http://www.nisc.go.jp/active/kihon/ts/bpc01_a.html）
○「セキュア・ジャパン 2006」（平成１８年６月　同会議）
（http://www.nisc.go.jp/active/kihon/pdf/sjf_2006.pdf）
○「セキュア・ジャパン 2007」（平成１９年６月　同会議）
（http://www.nisc.go.jp/active/kihon/pdf/sjf_2007.pdf）
○「セキュア・ジャパン 2008」（平成２０年６月　同会議）
（http://www.nisc.go.jp/active/kihon/pdf/sjf_2008.pdf）